REMARKS/ARGUMENTS

In response to the Examiner's further Office Action of January 3, 2008 issued with respect to the present RCE application, the Applicant respectfully submits the accompanying Amendment of the claims and the below Remarks.

Regarding Amendment

In the Amendment:

independent claim 1 is amended to replace the recitations of the "trusted" and "untrusted" authentication chips with --first-- and --second-- authentication chips, respectively, to consistently recite --secret-- random number and to specify that the plural and random number of times is determined based on a clock signal. Support for these amendments can be found, for example, at page 66, lines 17-27 of the present specification;

dependent claims 2, 4, 5, 7-9, 11, 12 and 17-19 are amended to conform with amended claim 1; and

dependent claims 10, 13, 14, 16 and 20 are unchanged.

It is respectfully submitted that the Amendment does not add any new matter to the present application.

Regarding Examiner's Note

It is respectfully submitted that the amendments of independent claim 1, and the claims dependent therefrom, clarify the nature of the "first" and "second" authentication chips, as is described at page 66, lines 17-27 of the present specification.

Regarding 35 USC 112, second paragraph Rejections

It is respectfully submitted that the amendments of independent claim 1, and the claims dependent therefrom, clarify the distinction between the recitations of the "secret random number" and the "plural and random number of times".

Regarding 35 USC 103(a) Rejections

It is respectfully submitted that the subject matter of amended independent claim 1, and claims 2, 4, 5, 7-14 and 16-20 dependent therefrom, is not taught or suggested by any one or more of previously cited Carmon, Sony, Spies, Goto and Schneier in view of newly cited Sibert (US 7,243,236), for at least the following reasons.

Independent claim 1 has been amended to specify that the plural and random number of times that the test function is called with a wrong number is determined based on a clock signal. In this way, the validity of the first chip is tested before the validity of the second chip is tested in a manner which is not ascertainable by an attacker (see page 66, lines 17-27 of the present specification).

As admitted by the Examiner, none of Carmon, Sony, Spies, Goto and Schneier teach or suggest calling a test function of an authentication chip with a wrong hash value a plural and random number of times.

Further, Sibert merely discloses process blocks 956-976 in which bytes of an application 600 are checked against a real hash value. Whilst the blocks 956-976 are disclosed as being repeated a random number of times, the manner of determining the actual

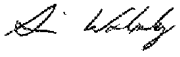
number of times is merely disclosed as being so that all of the bytes of the application are checked (see col. 25, lines 31-40).

Thus, it is respectfully submitted that since Sibert discloses checking against real hash values not wrong hash values, one of ordinary skill in the art would not have been motivated to combine Sibert and Goto (and the other cited references) as is contended by the Examiner. Further, even if this combination were made, because Sibert does not disclose or suggest basing determination of the random number of times on a clock signal, the claimed invention is not taught or suggested by the combined cited references.

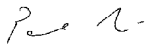
It is respectfully submitted that all of the Examiner's objections and rejections have been traversed. Accordingly, it is submitted that the present application is in condition for allowance and reconsideration of the present application is respectfully requested.

Very respectfully,

Applicant/s:



Simon Robert Walmsley



Paul Lapstun

C/o: Silverbrook Research Pty Ltd
393 Darling Street
Balmain NSW 2041, Australia

Email: kia.silverbrook@silverbrookresearch.com

Telephone: +612 9818 6633

Facsimile: +61 2 9555 7762